

---

## 4 OCTAVE Allegro Example Worksheets v1.0

This section contains example worksheets from an assessment of a hospital patient information database. The purpose of this example is to demonstrate what the OCTAVE Allegro worksheets generally look like when they are completed and to provide some additional insights into the assessment process. The example includes each of the first nine worksheets and a sampling of actual risks and associated mitigation plans (Worksheet 10). The example, however, does not include a set of completed threat questionnaires. The identified risks were generated from consideration of the questionnaires. For clarity, a consideration of the probability associated with a threat when considering risks and developing mitigation strategies is not included in this example.



Allegro Worksheet 1	RISK MEASUREMENT CRITERIA – REPUTATION AND CUSTOMER CONFIDENCE		
Impact Area	Low	Moderate	High
<i>Reputation (Staff)</i>	Reputation among non-physician hospital staff is minimally affected; little or no effort or expense is required to recover.	Reputation among non-physician hospital staff is damaged. No more than \$100K in time and effort required to recover.	Reputation among non-physician hospital staff is severely damaged. More than \$100K in time and effort required to recover. Relationship with staff is affecting reputation with physicians and community. Poor relationship affecting hospital efficiency and having noticeable effect on bed turnover rate.
<del>Customer Loss</del> <i>Reputation (Physicians)</i>	Reputation among physicians is minimally affected; little or no effort or expense is required to recover. Little or no change in hospital occupancy rate.	Reputation among physicians is damaged, causing physician population to reconsider sending patients to hospital. Occupancy rate changes of between one and five percent directly attributable to reputation problem. More than \$100K in time and effort required to recover.	Reputation among physicians is severely damaged. Critical staff physicians and hospital affiliated physicians are considering leaving. Occupancy changes of more than five percent are directly attributable to reputation problems. More than \$500K in time and effort required to recover.
<i>Other: Reputation (Community)</i>	Reputation in community from which hospital draws patients is minimally affected; little or no effort or expense is required to recover. Little or no change in hospital occupancy rate.	Reputation in community is damaged, causing potential patients to balk at doctor recommendations to the hospital. Occupancy rate changes of between one and five percent directly attributable to reputation. More than \$100K in time and effort required to recover.	Reputation in community is severely damaged, causing potential patients to refuse doctor recommendations to the hospital. Occupancy rate changes of more than five percent are directly attributable to reputation problem. More than \$500K in time and effort required to recover.
<i>Other: Occupancy Rates</i>	A reduction of the hospital occupancy rate of less than 2%	A reduction of the hospital occupancy rate of between 2% and 5%	A reduction of the hospital occupancy rate of more than 5%



Allegro Worksheet 2	RISK MEASUREMENT CRITERIA – FINANCIAL		
Impact Area	Low	Moderate	High
<i>Operating Costs</i>	Increase of less than 2.5% in annual operating costs	Increase of between 2.5% and 5% in annual operating costs	Increase of more than 5% in annual operating costs
<i>Revenue Loss</i>	Less than \$100K reduction in yearly revenue loss	Between \$100K and \$1M in yearly revenue loss	More than \$1M in yearly revenue loss
<i>One-Time Financial Loss</i>	Less than \$100K reduction in yearly revenue loss	Between \$100K and \$1M in yearly revenue loss	More than \$1M in yearly revenue loss
<i>Other:</i>			



Allegro Worksheet 3	RISK MEASUREMENT CRITERIA – PRODUCTIVITY		
Impact Area	Low	Moderate	High
<i>Staff Hours</i>	Staff work hours increase labor costs by less than \$100K.	Staff work hours increase labor costs between \$100K and \$1M.	Staff work hours increase labor costs by more than \$1M.
<i>Other: Bed Turnover Rate</i>	Turnover rate for hospital beds decreases less than 2%.	Turnover rate for hospital beds decreases between 2% and 5%.	Turnover rate for hospital beds decreases by more than 5%.
<i>Other:</i>			
<i>Other:</i>			





Allegro Worksheet 4	RISK MEASUREMENT CRITERIA – SAFETY AND HEALTH		
Impact Area	Low	Moderate	High
<i>Life</i>	No loss or significant threat to customers' or staff members' lives and no regulatory response.	Customers' or staff members' lives are threatened, but they will recover after receiving medical treatment. Only minimal regulatory response and less than \$250K in related costs.	Loss of customers' or staff members' lives. Significant regulatory response, lawsuits, and more than \$250K in related costs.
<i>Health</i>	Minimal, immediately treatable degradation in customers' or staff members' health with recovery within days. Minimal regulatory response and less than \$100K in related costs.	Temporary or recoverable impairment of customers' or staff members' health. Only minimal regulatory response and between \$250 and \$500K in related recovery costs.	Permanent impairment of significant aspects of customers' or staff members' health. Significant regulatory response involving investigations and more than \$500K in recovery costs.
<i>Safety</i>	Safety questioned, but no regulatory response and little to no economic cost.	Safety affected, minimal regulatory response, and less \$250K in recovery costs.	Safety violated, significant regulatory response involving investigations, and more than \$250K in recovery and response costs.
<i>Other:</i>			



**Allegro Worksheet 5****RISK MEASUREMENT CRITERIA – FINES AND LEGAL PENALTIES**

Impact Area	Low	Moderate	High
<i>Fines</i>	Fines less than \$100K are levied.	Fines between \$100K and \$250K are levied.	Fines greater than \$500K are levied.
<i>Lawsuits</i>	Non-frivolous lawsuit or lawsuits less than \$100K are filed against the organization, or frivolous lawsuit(s) are filed against the organization.	Non-frivolous lawsuit or lawsuits between \$100K and \$1M are filed against the organization.	Non-frivolous lawsuit or lawsuits greater than \$1M are filed against the organization.
<i>Investigations</i>	No queries from government or other investigative organizations.	Government or other investigative organization requests information or records (low profile).	Government or other investigative organization initiates a high-profile, in-depth investigation into organizational practices.
<i>Other:</i>			



**Allegro Worksheet 6****RISK MEASUREMENT CRITERIA – USER DEFINED**

<b>Impact Area</b>	<b>Low</b>	<b>Moderate</b>	<b>High</b>



Allegro Worksheet 7		IMPACT AREA PRIORITIZATION WORKSHEET
PRIORITY	IMPACT AREAS	
2	Reputation and Customer Confidence	
4	Financial	
3	Productivity	
5	Safety and Health	
1	Fines and Legal Penalties	
n/a	User Defined	





Allegro Worksheet 8	CRITICAL INFORMATION ASSET PROFILE	
(1) Critical Asset	(2) Rationale for Selection	(3) Description
<i>What is the critical information asset?</i>	<i>Why is this information asset important to the organization?</i>	<i>What is the agreed-upon description of this information asset?</i>
Patient Billing and Collection Data (PBCD)	Keeping accurate billing records is essential for negotiating and collecting compensation from insurance organizations. Challenges to bills from insurance organizations can force the hospital to absorb billing differences. Challenges can also significantly delay the time between services being rendered and compensation being received by the hospital.	This information asset contains all of the information necessary to bill a patient and his/her insurance company for treatment/services received from the hospital. This includes patient demographic information (names, addresses, social security numbers, and insurance carriers), treatment/service history and associated billing codes, and payment histories.
(4) Owner(s)		
<i>Who owns this information asset?</i>		
The owner of this information asset is the Director of Patient Billing and Collection (Todd Marnivich).		
(5) Security Requirements		
<i>What are the security requirements for this information asset?</i>		
<input type="checkbox"/> Confidentiality	Only authorized personnel can view this information asset, as follows:	Members of the hospital financial staff responsible for billing and collection should have "read" access to individual records. Other financial staff can have access to summary information. Data entry personnel should have "read" access to individual records.

<input type="checkbox"/> Integrity	Only authorized personnel can modify this information asset, as follows:	Only authorized data entry personnel and members of the hospital financial staff may update/change billing record information. Billing records should only be updated with the actual billable services provided to the patient.	
<input type="checkbox"/> Availability	This asset must be available for these personnel to do their jobs, as follows:	The PBCD must be available to data entry personnel for updates to billing and procedures codes and for admitting purposes. The PBCD must be available to financial staff for billing and collection activities.	
	This asset must be available for <b>24</b> hours, <b>7</b> days/week, <b>52</b> weeks/year.	The PBCD information asset should be available 24x7 as procedures are ordered around the clock at the hospital. It must be available to the financial staff (specifically the patient billing and collection staff) during regular business hours. Short outages would not cause significant problems but extended outages (more than 8 hours) would cause a significant backlog.	
<input type="checkbox"/> Other	This asset has special regulatory compliance protection requirements, as follows:	Because these billing records contain patient treatment information, they are subject to HIPAA regulations.	
<b>(6) Most Important Security Requirement</b> <i>What is the most important security requirement for this information asset?</i>			
<input type="checkbox"/> Confidentiality	<input checked="" type="checkbox"/> Integrity	<input type="checkbox"/> Availability	<input type="checkbox"/> Other

Allegro Worksheet 9a		INFORMATION ASSET RISK ENVIRONMENT MAP (TECHNICAL)	
INTERNAL			
CONTAINER DESCRIPTION		OWNER(S)	
1. The PBCD primarily resides on the patient billing management system (PBMS) which consists of <u>two database servers</u> and <u>three application/web servers</u> . This is a vendor proprietary system that provides a web interface for authorized personnel to access/manipulate entries. The underlying operating system is Windows Server 2003.		Managed by hospital IT department.	
2. <u>Hospital internal network</u> . All transactions to and from the PBCD system travel on this network.		Managed by hospital IT department.	
3. <u>Hospital workstations</u> (e.g., order entry workstations, finance department workstations, and hospital admitting workstations).		Managed by hospital IT department.	
EXTERNAL			
CONTAINER DESCRIPTION		OWNER(S)	
1. <u>The Internet</u> . Most bills are electronically shipped in bulk to insurance providers each week. Once billing information arrives at the insurance company, the insurance company is considered to be the owner of the information asset.		Unknown	
2.			
3.			
4.			



Allegro Worksheet 9b		INFORMATION ASSET RISK ENVIRONMENT MAP (PHYSICAL)	
INTERNAL			
CONTAINER DESCRIPTION		OWNER(S)	
1. <u>Paper copies</u> of billing summaries, statements, and histories are regularly printed and kept by members of finance department.		Financial staff	
2. <u>Backup tapes</u> of PBCD are created each night and kept onsite until regular pickup by storage vendor.		Managed by hospital IT department.	
3.			
4.			
EXTERNAL			
CONTAINER DESCRIPTION		OWNER(S)	
1. <u>Paper copies of billing statements</u> are regularly printed and mailed to patients.		Financial staff	
2. <u>Paper copies of billing statements, summaries, histories, and reports</u> are regularly printed and mailed to insurance providers.		Financial Staff	
3.			
4.			



INTERNAL PERSONNEL	
NAME OR ROLE/RESPONSIBILITY	DEPARTMENT OR UNIT
1. Admitting staff	Admissions
2. Order entry staff	Business Services
3. Financial staff	Business Services
4. Hospital messenger service staff	Business Services
EXTERNAL PERSONNEL	
CONTRACTOR, VENDOR, ETC.	ORGANIZATION
1. Insurance organization's claims staff	Hospital Insurance, Inc.
2. Third-party vendor manages the transportation and storage of backup tapes for the PBCD system. Relationship is managed via the hospital IT department.	Safe-N-Secure Data Storage, Inc.
3.	
4.	





Allegro Worksheet 10		INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk	Threat	Information Asset	PBCD		
		Area of Concern	Patient billing data is altered when unauthorized individual gains access to PBMS system. (A vulnerability in the Windows 2003 Server operating system is leveraged to gain administrative access to the PBMS system.)		
		(1) Actor <i>Who would exploit the weakness?</i>	Disgruntled current employees		
		(2) Means <i>How would the actor do it? What would they do?</i>	Using workstation on the internal hospital network, employee launches attack on PBMS system.		
		(3) Motive <i>What is the actor's reason for doing it?</i>	Wants to harm hospital because of ongoing labor contract disputes		
		(4) Outcome <i>What would be the resulting effect on the information asset?</i>	<input type="checkbox"/> Disclosure <input type="checkbox"/> Destruction <input checked="" type="checkbox"/> <b>Modification</b> <input type="checkbox"/> Interruption		
		(5) Security Requirements <i>How would the information asset's security requirements be breached?</i>	Only authorized members of the hospital data entry staff and finance staff should be able to modify PBCD asset.		
	(6) Probability <i>What is the likelihood that this threat scenario could occur?</i>	<input type="checkbox"/> High	<input type="checkbox"/> Medium	<input type="checkbox"/> Low	
	(7) Consequences <i>What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?</i>	(8) Severity <i>How severe are these consequences to the organization or asset owner by impact area?</i>			
		Impact Area	Value	Score	
If the intruder goes unnoticed, significant financial harm could come to the hospital. If insurance companies are not charged for services, the hospital would lose money. If the insurance companies are over-charged or charged for services not rendered, there will be additional financial repercussions.	Reputation & Customer Confidence	Low	2		
	Financial	High	12		
	Productivity	High	9		
	Safety & Health	Low	5		
	Fines & Legal Penalties	Med	2		
	User Defined Impact Area				
Significant labor charges will be required to audit and re-enter billing data.					
Exposure of patient data may lead to fines and possible lawsuits.					
Relative Risk Score			30		

## (9) Risk Mitigation

Based on the total score for this risk, what action will you take?

☐ Accept

☐ Defer

☒ Mitigate

☐ Transfer

For the risks that you decide to mitigate, perform the following:

On what container  
would you apply con-  
trols?

What administrative, technical, and physical controls would you apply on this container?  
What residual risk would still be accepted by the organization?

Hospital network

- Restrict network traffic to ensure that only the workstations of authorized users can access PBMS.
- Restrict network traffic to ensure that only valid PBMS transaction traffic can reach the PBMS system. This reduces the number of places from which attacks can be launched against the system and the types of attacks. Asset would still be vulnerable to services that remain exposed.

PBMS

- Ensure that transaction auditing is enabled so that improper transactions can be identified and backed out of the system. This control relies on the integrity of the audit log—if it were to be destroyed, it would be impossible to back out transactions.

PBMS

- Ensure that PBMS system and the underlying OS/applications are up-to-date with security patches. This control reduces the exposure against known attacks but does nothing to limit unknown vulnerabilities.

Allegro Worksheet 10		INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk	Threat	Information Asset	PBCD		
		Area of Concern	Patient information is disclosed to unauthorized individuals, opening hospital to possible HIPAA violations and lawsuits. (PBCD travels on hospital intranet in the clear between workstations and PBMS System.)		
		(1) Actor <i>Who would exploit the weakness?</i>	An employee with access to hospital network		
		(2) Means <i>How would the actor do it? What would they do?</i>	A network administrator captures traffic on network switching device.		
		(3) Motive <i>What is the actor's reason for doing it?</i>	Curiosity about a patient		
		(4) Outcome <i>What would be the resulting effect on the information asset?</i>	<input checked="" type="checkbox"/> Disclosure <input type="checkbox"/> Destruction <input type="checkbox"/> Modification <input type="checkbox"/> Interruption		
		(5) Security Requirements <i>How would the information asset's security requirements be breached?</i>	Only authorized personnel can view this information as-set.		
	(6) Probability <i>What is the likelihood that this threat scenario could occur?</i>	<input type="checkbox"/> High	<input type="checkbox"/> Medium	<input type="checkbox"/> Low	
	(7) Consequences <i>What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?</i>		(8) Severity <i>How severe are these consequences to the organization or asset owner by impact area?</i>		
	Exposure of patient sensitive information opens the hospital to lawsuits and fines for breaches of HIPAA regulations.  The public's overall perception of the hospital's quality could be negatively affected if patient sensitive information is publicized.		Impact Area	Value	Score
Reputation & Customer Confidence			Med	4	
Financial			Low	4	
Productivity			Low	3	
Safety & Health			Low	5	
Fines & Legal Penalties			Med	2	
		User Defined Impact Area			
Relative Risk Score				18	

(9) Risk Mitigation	
Based on the total score for this risk, what action will you take?	
<input type="checkbox"/> Accept	<input type="checkbox"/> Defer
<input checked="" type="checkbox"/> Mitigate	<input type="checkbox"/> Transfer
For the risks that you decide to mitigate, perform the following:	
On what container would you apply controls?	What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?
PBMS	<ul style="list-style-type: none"> <li>Enable SSL encryption on connections on PBMS server. This will reduce exposure to network captures by introducing end to end encryption on PBMS transactions.</li> </ul>
Hospital Network	<ul style="list-style-type: none"> <li>Enable logging of consoles of networking devices and enact policy to ensure that logs are regularly reviewed. This will reduce likelihood of insider activity and increase the likelihood that outsider activity will be detected.</li> </ul>

Allegro Worksheet 10		INFORMATION ASSET RISK WORKSHEET				
Information Asset Risk	Threat	Information Asset	PBCD			
		Area of Concern	Denial-of-service attack against hospital network impedes the hospital's ability to electronically deliver bills to the insurance organizations. (PBCD must traverse Internet to reach insurance organizations.)			
		(1) Actor <i>Who would exploit the weakness?</i>	A hacker who wants to see if he can damage the hospital financially			
		(2) Means <i>How would the actor do it? What would they do?</i>	Uses DoS toolkit found on hacking website			
		(3) Motive <i>What is the actor's reason for doing it?</i>	Entertainment			
		(4) Outcome <i>What would be the resulting effect on the information asset?</i>	<input type="checkbox"/> Disclosure <input type="checkbox"/> Destruction <input type="checkbox"/> Modification <input checked="" type="checkbox"/> <b>Interruption</b>			
		(5) Security Requirements <i>How would the information asset's security requirements be breached?</i>	The PBCD must be available for billing and collection activities.			
		(6) Probability <i>What is the likelihood that this threat scenario could occur?</i>	<input type="checkbox"/> High	<input type="checkbox"/> Medium	<input type="checkbox"/> Low	
	(7) Consequences <i>What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?</i>	(8) Severity <i>How severe are these consequences to the organization or asset owner by impact area?</i>				
	Continual attacks against hospital network add significant delays in the reimbursement process. Hospital must burn CDROMs with the data and messenger them to insurance services. Significant financial and productivity impacts.	Impact Area	Value	Score		
		Reputation & Customer Confidence	Med	4		
		Financial	High	12		
Productivity		High	9			
Safety & Health		Low	5			
Fines & Legal Penalties		Low	1			
	User Defined Impact Area					
Relative Risk Score					31	

<b>(9) Risk Mitigation</b>	
<i>Based on the total score for this risk, what action will you take?</i>	
<input type="checkbox"/> Accept	<input type="checkbox"/> Defer
<input checked="" type="checkbox"/> Mitigate	<input type="checkbox"/> Transfer
<b>For the risks that you decide to mitigate, perform the following:</b>	
<i>On what container would you apply controls?</i>	<i>What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?</i>
Internet	<ul style="list-style-type: none"> <li>Find a new service provider who has more robust connectivity solutions and can be more supportive in preventing DoS attacks.</li> </ul>
Internet	<ul style="list-style-type: none"> <li>Work with insurance companies to develop alternative delivery methods such as a direct connection.</li> </ul>

Allegro Worksheet 10		INFORMATION ASSET RISK WORKSHEET		
Information Asset Risk	Information Asset	PBCD		
	Area of Concern	An unauthorized individual is able to view PBCD asset and exposes it to others. (Data entry staff member walks away from workstation connected to PBMS server that is located in a public area of the hospital and thus is freely accessible by patients, other hospital staff, or visitors.)		
	Threat	(1) Actor <i>Who would exploit the weakness?</i>	Hospital staff and/or inquisitive patients or hospital visitors	
		(2) Means <i>How would the actor do it? What would they do?</i>	When no one is at the workstation, a hospital worker, patient, or visitor could sit down in front of it and begin to access data.	
		(3) Motive <i>What is the actor's reason for doing it?</i>	Curiosity about famous patient on another floor or general curiosity	
		(4) Outcome <i>What would be the resulting effect on the information asset?</i>	<input checked="" type="checkbox"/> Disclosure <input type="checkbox"/> Destruction <input type="checkbox"/> Modification <input type="checkbox"/> Interruption	
		(5) Security Requirements <i>How would the information asset's security requirements be breached?</i>	Only authorized personnel can view this information asset.	
		(6) Probability <i>What is the likelihood that this threat scenario could occur?</i>	<input type="checkbox"/> High	<input type="checkbox"/> Medium
	(7) Consequences <i>What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?</i>	(8) Severity <i>How severe are these consequences to the organization or asset owner by impact area?</i>		
	Exposure of patient sensitive information opens the hospital to lawsuits and fines for breaches of HIPAA regulations.	Impact Area	Value	Score
Reputation & Customer Confidence		High	6	
Financial		Med	4	
The public's overall perception of the hospital's quality could be negatively affected if patient sensitive information is publicized.		Productivity	Low	3
		Safety & Health	Low	5
		Fines & Legal Penalties	Med	2
	User Defined Impact Area			
Relative Risk Score			20	

<b>(9) Risk Mitigation</b>	
<i>Based on the total score for this risk, what action will you take?</i>	
<input type="checkbox"/> Accept	<input type="checkbox"/> Defer
<input checked="" type="checkbox"/> Mitigate	<input type="checkbox"/> Transfer
<b>For the risks that you decide to mitigate, perform the following:</b>	
<i>On what container would you apply controls?</i>	<i>What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?</i>
Hospital workstations	<ul style="list-style-type: none"> <li>Force automatic screen locking for workstations that have been idle for more than five minutes. This would reduce the exposure of the data when workstation is unattended to a much smaller time period.</li> </ul>
PBMS	<ul style="list-style-type: none"> <li>Enable transaction logging on the PBMS system. This would allow the hospital to determine accountability after the fact and could possibly lessen the impact of possible lawsuits and fines.</li> </ul>
PBMS	<ul style="list-style-type: none"> <li>Enable controls in PBMS system to restrict access of data entry staff to only those patients in their specialty group. This will limit the exposure of patient data to only the patient information that the data entry staff is likely to encounter in performing their job functions.</li> </ul>
Admit staff	<ul style="list-style-type: none"> <li>Provide regular refresher training for the admit staff on the responsibilities for protecting patient data and on HIPAA rules and regulations.</li> <li>Enact policy that all admit staff must sign non-disclosure agreement with the hospital.</li> </ul>
Data entry staff	<ul style="list-style-type: none"> <li>Provide regular refresher training for the data entry staff on the responsibilities for protecting patient data and on HIPAA rules and regulations.</li> <li>Enact policy that all data-entry staff must sign non-disclosure agreement with the hospital.</li> </ul>
Financial staff	<ul style="list-style-type: none"> <li>Provide regular refresher training for the financial staff on the responsibilities for protecting patient data and on HIPAA rules and regulations.</li> <li>Enact policy that all financial staff must sign non-disclosure agreement with the hospital.</li> </ul>



Allegro Worksheet 10		INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk	Threat	Information Asset	PBCD		
		Area of Concern	Paper copies of billing statements are found by an unauthorized individual and patient sensitive data is exposed. (Financial staff members regularly produce paper copies of billing summaries and leave them on their desks.)		
		(1) Actor <i>Who would exploit the weakness?</i>	Janitorial staff		
		(2) Means <i>How would the actor do it? What would they do?</i>	Sees billing summary while cleaning an office		
		(3) Motive <i>What is the actor's reason for doing it?</i>	Curiosity		
		(4) Outcome <i>What would be the resulting effect on the information asset?</i>	<input checked="" type="checkbox"/> Disclosure <input type="checkbox"/> Destruction <input type="checkbox"/> Modification <input type="checkbox"/> Interruption		
		(5) Security Requirements <i>How would the information asset's security requirements be breached?</i>	Only authorized personnel can view this information as-set.		
	(6) Probability <i>What is the likelihood that this threat scenario could occur?</i>	<input type="checkbox"/> High	<input type="checkbox"/> Medium	<input type="checkbox"/> Low	
	(7) Consequences <i>What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?</i>	(8) Severity <i>How severe are these consequences to the organization or asset owner by impact area?</i>			
	Exposure of patient sensitive information opens the hospital to lawsuits and fines for breaches of HIPAA regulations.  The public's overall perception of the hospital's quality could be negatively affected if patient sensitive information is publicized.	Impact Area	Value	Score	
Reputation & Customer Confidence		Med	4		
Financial		Low	4		
Productivity		Low	3		
Safety & Health		Low	5		
Fines & Legal Penalties		Med	2		
User Defined Impact Area					
Relative Risk Score			18		

[illegible]

Allegro Worksheet 10		INFORMATION ASSET RISK WORKSHEET				
Information Asset Risk	Threat	Information Asset	PBCD			
		Area of Concern	Backup tapes lost and unable to recover transactions. (Only one set of backup tapes is currently being created and stored off site.)			
		(1) Actor <i>Who would exploit the weakness?</i>	Third-party backup storage provider			
		(2) Means <i>How would the actor do it? What would they do?</i>	Shipment of backup tapes is lost in storage.			
		(3) Motive <i>What is the actor's reason for doing it?</i>	Accidental			
		(4) Outcome <i>What would be the resulting effect on the information asset?</i>	<input type="checkbox"/> Disclosure <input checked="" type="checkbox"/> Destruction <input type="checkbox"/> Modification <input type="checkbox"/> Interruption			
		(5) Security Requirements <i>How would the information asset's security requirements be breached?</i>	Only authorized personnel can view this information as-set.			
		(6) Probability <i>What is the likelihood that this threat scenario could occur?</i>	<input type="checkbox"/> High	<input type="checkbox"/> Medium	<input type="checkbox"/> Low	
		(7) Consequences <i>What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?</i>		(8) Severity <i>How severe are these consequences to the organization or asset owner by impact area?</i>		
				Impact Area	Value	Score
		If there is a system crash and the hospital is unable to recall backup tapes to restore transactions, then all transaction will need to be restored from paper patient records.		Reputation & Customer Confidence	Low	2
				Financial	High	12
There would be significant financial and productivity impacts to restore transaction.		Productivity	High	9		
		Safety & Health	Low	5		
Likely that during the restoration process many charges would be overlooked or incorrectly added. There would be losses for the missing charges and possibly increased reimbursement time as insurance companies disputed incorrect charges.		Fines & Legal Penalties	Low	1		
		User Defined Impact Area				
Relative Risk Score					31	

## (9) Risk Mitigation

Based on the total score for this risk, what action will you take?

☐ Accept

☐ Defer

☒ Mitigate

☐ Transfer

For the risks that you decide to mitigate, perform the following:

On what container  
would you apply con-  
trols?

What administrative, technical, and physical controls would you apply on this con-  
tainer? What residual risk would still be accepted by the organization?

Backup tapes

- Simply add a backup run and keep second copy of the backup tapes stored on site. Keeping a second copy of re-  
cent tapes on site will provide some redundancy but will not  
completely remove risk of being able to restore old trans-  
actions.

Information Asset Risk	Threat	Information Asset	PBCD		
		Area of Concern	Billing statement sent to wrong patient address. (Envelopes get out of order and wrong address label is applied and information in bill is not encrypted.)		
		(1) Actor <i>Who would exploit the weakness?</i>	Hospital financial staff		
		(2) Means <i>How would the actor do it? What would they do?</i>	Envelopes get shuffled between machines.		
		(3) Motive <i>What is the actor's reason for doing it?</i>	Accidental		
		(4) Outcome <i>What would be the resulting effect on the information asset?</i>	<input checked="" type="checkbox"/> Disclosure <input type="checkbox"/> Destruction <input type="checkbox"/> Modification <input type="checkbox"/> Interruption		
		(5) Security Requirements <i>How would the information asset's security requirements be breached?</i>	Only authorized personnel can view this information asset.		
	(6) Probability <i>What is the likelihood that this threat scenario could occur?</i>	<input type="checkbox"/> High	<input type="checkbox"/> Medium	<input type="checkbox"/> Low	
	(7) Consequences <i>What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?</i>		(8) Severity <i>How severe are these consequences to the organization or asset owner by impact area?</i>		
	Exposure of patient sensitive information opens the hospital to lawsuits and fines for breaches of HIPAA regulations.  The public's overall perception of the hospital's quality could be negatively affected if patient sensitive information is publicized.		Impact Area	Value	Score
			Reputation & Customer Confidence	Low	2
			Financial	Low	4
			Productivity	Low	3
			Safety & Health	Low	5
			Fines & Legal Penalties	Low	1
			User Defined Impact Area		
Relative Risk Score					15

#### (9) Risk Mitigation

<i>Based on the total score for this risk, what action will you take?</i>			
<input type="checkbox"/> Accept	<input checked="" type="checkbox"/> <b>Defer</b>	<input type="checkbox"/> Mitigate	<input type="checkbox"/> Transfer
<b>For the risks that you decide to mitigate, perform the following:</b>			
<i>On what container would you apply controls?</i>	<i>What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?</i>		

Allegro Worksheet 10		INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk	Threat	Information Asset	PBCD		
		Area of Concern	Procedures not performed on a patient are added to billing summary. (No one checks that the data entry staff enters the correct procedures from the chart unless the insurance company complains about a charge.)		
		(1) Actor <i>Who would exploit the weakness?</i>	Disgruntled data entry staff		
		(2) Means <i>How would the actor do it? What would they do?</i>	Enters codes for test and procedures that were never performed		
		(3) Motive <i>What is the actor's reason for doing it?</i>	Wants to harm the hospital		
		(4) Outcome <i>What would be the resulting effect on the information asset?</i>	<input type="checkbox"/> Disclosure <input type="checkbox"/> Destruction <input checked="" type="checkbox"/> <b>Modification</b> <input type="checkbox"/> Interruption		
		(5) Security Requirements <i>How would the information asset's security requirements be breached?</i>	Billing records should only be updated with the actual billable services provided to the patient.		
	(6) Probability <i>What is the likelihood that this threat scenario could occur?</i>	<input type="checkbox"/> High	<input type="checkbox"/> Medium	<input type="checkbox"/> Low	
	(7) Consequences <i>What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?</i>		(8) Severity <i>How severe are these consequences to the organization or asset owner by impact area?</i>		
	<b>If the activity goes unnoticed, significant financial harm could come to the hospital. If patients are charged for services the hospital did not deliver, the hospital would have to return money and might be sued for additional damages or negligence.</b>  <b>Significant labor charges will be required to audit and re-enter billing data.</b>  <b>Insurance companies will likely take longer in reviewing and providing compensation to the hospital. This could cause a significant interruption in hospital's cash flow.</b>		Impact Area	Value	Score
Reputation & Customer Confidence			Med	8	
Financial			High	12	
Productivity			High	9	
Safety & Health			Low	5	
Fines & Legal Penalties			High	3	
		User Defined Impact Area			
Relative Risk Score				37	

[illegible]



